

ABSTRACT OF THE DISCLOSURE

Disclosed is an RR (Return Routability) method for secure communication that improves security by eliminating the threat of a man in the middle attack. A mobile node transmits an HoTI (Home Test Init) packet to the home agent, and transmits a CoTI (Care of Test Init) packet to the corresponding node. A home agent transmits the HoTI packet including first key information generated by a specified method to a corresponding node, and the corresponding node transmits an HoT (Home of Test) packet including second key information generated by a specified method to the home agent and transmits a CoT (Care-of Test) packet encrypted using a secret key generated from the first key information by a specified method to the mobile node. The home agent transmits the secret key generated from the received HoT packet by the specified method to the mobile node, and the mobile node decodes the received encrypted CoT packet using the received secret key.